IN THE UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION

JUANITA KIRKSEY, *individually & on behalf of all others similarly situated*, Plaintiff, v. THE CHARLOTTE-MECKLENBURG HOSPITAL AUTHORITY (d/b/a ATRIUM HEALTH), Defendant.	Case No. _____ **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Juanita Kirksey, individually and on behalf of all others similarly situated, by and through undersigned counsel, hereby alleges the following against Defendant The Charlotte-Mecklenburg Hospital Authority (d/b/a Atrium Health) ("**Atrium**" or "**Defendant**"). Facts pertaining to Plaintiff and her experiences and circumstances are alleged based upon personal knowledge and all other facts herein are alleged based upon the investigation of counsel and, where indicated, upon information and good faith belief.

NATURE OF THE ACTION

1. Plaintiff brings this class action lawsuit against Atrium for its failure to properly secure and safeguard Plaintiff's and other similarly situated current and former Atrium patients' (collectively defined herein as the "Class" or "Class Members") personally identifiable information ("PII") and protected health information ("PHI"), including names, dates of birth, Social Security numbers, Driver's licenses, health and health insurance information, and financial data (collectively, the "Private Information") from cybercriminals.

2. Defendant Atrium is a healthcare organization and hospital network offering a wide range of clinical services to patients across multiple states.[1] Defendant operates 40 hospitals, 7 emergency departments, 30 urgent care centers and approximately 1400 additional care locations throughout North Carolina, South Carolina, Georgia and Alabama.

3. As part of its healthcare business, Atrium collects a treasure-trove of data from its patients, including highly sensitive Private Information.

4. Healthcare providers that handle Private Information have an obligation to employ reasonable and necessary data security practices to protect the sensitive, confidential and personal information entrusted to them.

5. This duty exists because it is foreseeable that the exposure of such Private Information to unauthorized persons—and especially hackers with nefarious intentions—will result in harm to the affected individuals, including, but not limited to, medical and financial identity theft, invasion of their private health matters and other long-term issues.

6. The harm resulting from a data and privacy breach manifests in several ways, including identity theft and financial and medical fraud, and the exposure of a person's Private Information through a data breach ensures that such person will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of their lives.

7. Mitigating that risk—to the extent it is even possible to do so—requires individuals to devote significant time, money and other resources to closely monitor their credit, financial

[1] *Atrium Health 2019 Annual Report,* https://atriumhealth.org/files/build_annual_report/index.html (last visited Sept. 18, 2024).

accounts, health records and email accounts, as well as to take a number of additional prophylactic measures.

8. In this instance, all of that could have been avoided if Atrium—which serves more than 34,000 patients a day across the Atrium network—had employed reasonable and appropriate data security measures.[2]

9. On or around September 13, 2024, Atrium announced that its patients' Private Information stored on its systems had been compromised by a phishing attack on several employee email accounts (the "Data Breach").[3]

10. Atrium allegedly indicated that the information impacted by the Data Breach included "an individual's first and/or last name; middle initial; street address, email address and/or phone number(s); Social Security number; date of birth; medical record number; certain government or employer identifiers; driver's license or state-issued identification number; bank or financial account numbers or information, including routing numbers, financial institution name, or expiration date; treatment/diagnosis, provider name, prescription, health insurance or treatment cost information; patient identification number; health insurance account or policy number(s); incidental health references; billing identification numbers; access credentials; and/or digital signatures."[4]

---

[2] *See id.*

[3] *See* JDSupra, *Atrium Health Confirms Report of Data Breach Stemming from Email Phishing Attack* (Sept. 17, 2024) (last visited Sept. 18, 2024); *see also* The HIPAA Journal, *Email Accounts Compromised in Atrium Health Phishing Attack* (Sept. 16, 2024), https://www.hipaajournal.com/atrium-health-phishing-attack/ (last visited Sept. 18, 2024).

[4] *See* Atrium Health, *A Notice to our Patients*, https://cdn.atriumhealth.org/-/media/documents/substitute-notices/atrium-health--charlotte-bec--substitute-notice-final.pdf?rev=c6bed3cc96eb4694b4a578c73fd0fca1&hash=58A4D4F600E2F7C506933E7A53BA1FD9 (last visited Sept. 18, 2024).

11. This is one of the most egregious data breaches of recent years as it appears that the Data Breach took place *in April 2024*[5] and in the months to come Atrium has gone to extraordinary lengths to conceal the details of the breach, including the number of affected victims and the exact categories of stolen data.

12. The only publicly available information regarding the Data Breach from Atrium itself is "A Notice to Our Patients" on Atrium's website (the "Incident Statement").[6] It appears that this statement was issued on or around September 13, 2024.

13. The exceedingly vague Statement does not provide any details about the Data Breach, stating only that "[t]he forensic consultant's analysis of the affected accounts, completed on July 17, 2024, indicates that the unauthorized party was not focused on email content pertaining to medical or health information."[7]

14. Atrium has not reported the Data Breach to the Department of Health and Human Services Office for Civil Rights ("HHS"), or any of the state agencies as of the filing of this complaint.

15. Thus, despite discovering the Data Breach on or around April 2023, Atrium still has not disclosed the full scope of the Data Breach or the information impacted, *or over four months after the fact.*

---

[5] *See supra*, note 3.

[6] *See* https://cdn.atriumhealth.org/-/media/documents/substitute-notices/atrium-health--charlotte-bec--substitute-notice-final.pdf?rev=c6bed3cc96eb4694b4a578c73fd0fca1&hash=58A4D4F600E2F7C506933E7A53BA1FD9 (last visited Sept. 18, 2024).

[7] *See supra*, note 4.

16. Defendant's Incident Statement is inadequate for several reasons. Omitted from Atrium's Statement were the number of affected victims, exact patient data accessed by cybercriminals, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their Private Information remains protected.

17. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach's critical facts. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach has been severely diminished.

18. As a direct and proximate result of Defendant's failure to implement and to follow basic security procedures, Plaintiff's and Class Members' PII and PHI is now in the hands of cybercriminals.

19. Plaintiff and Class Members are now at a significantly increased and certainly impending risk of fraud, identity theft, misappropriation of health insurance benefits, intrusion of their health privacy and similar forms of criminal mischief, risk which may last for the rest of their lives.

20. Consequently, Plaintiff and Class Members must devote substantially more time, money and energy to protect themselves, to the extent possible, from these crimes. *See McMorris v. Lopez*, 995 F.3d 295, 301 (2d Cir. 2021) (quoting *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015) ("Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities.")).

21. Plaintiff, on behalf of herself and all others similarly situated, therefore brings claims for (i) Negligence; (ii) Breach of Implied Contract; (iii) Breach of the Implied Covenant of Good Faith and Fair Dealing; (iv) Unjust Enrichment; and (v) Declaratory Judgment. Plaintiff seeks damages and injunctive relief, including the adoption of reasonably necessary and appropriate data security practices to safeguard the Private Information in Defendant's custody in order to prevent incidents like the Data Breach from occurring in the future.

PARTIES

22. Plaintiff Juanita Kirksey is, and at all times mentioned herein, was an individual citizen residing in Stokes County, North Carolina and has been a patient of Atrium for several years.

23. Plaintiff understandably and reasonably believed and trusted that her Private Information provided to Atrium would be kept confidential and secure and would be used solely for authorized purposes.

24. Defendant The Charlotte-Mecklenburg Hospital Authority (d/b/a Atrium Health) is a healthcare service provider. Defendant is incorporated in North Carolina with its principal place of business located at 1000 Blythe Boulevard in Charlotte, North Carolina 28203.

JURISDICTION & VENUE

25. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of $5,000,000 exclusive of interest and costs, there are more than 100 putative class members and minimal diversity exists because at least one putative class member is a citizen of a different state than Defendant.

26. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

27. This Court has personal jurisdiction over Atrium because it operates and maintains its principal place of business in this District. Further, Atrium is authorized to and regularly conduct business in this District and make decisions regarding corporate governance and management of its business operations in this District, including decisions regarding the security of patients' Private Information.

28. Venue is proper in this District under 28 U.S.C. § 1391(a)(1) through (d) because: a substantial part of the events giving rise to this action occurred in this District and Atrium has harmed Class Members residing in this District.

COMMON FACTUAL ALLEGATIONS

A. Atrium Collects a Significant Amount of Private Information.

29. Atrium Health is a healthcare system operating across North Carolina, South Carolina, Georgia and Alabama.

30. The Atrium network has 40 hospitals and more than 1,400 locations across several states.

31. In 2019 Atrium officially combined with Georgia-based Navicent Health.[8]

32. Also in 2019 Atrium announced plans to combine with Wake Forest Baptist Health and Wake Forest University to create an academic healthcare system, including a School of Medicine campus in Charlotte, as well as signed a letter of intent to create a strategic combination with Georgia-based Floyd Health System.[9]

[8] *See* https://atriumhealth.org/files/build_annual_report/index.html?
[9] *See id.*

33. As a condition of receiving medical services from Atrium, patients are required to entrust it with highly sensitive personal and health information.

34. While providing healthcare services, Defendant receives, creates and handles an incredible amount of Private Information, including, *inter alia*, names, addresses, dates of birth, addresses, phone numbers, email addresses, Social Security numbers and medical information such as dates of service, diagnosis/treatment information, medical billing/claims information, health insurance information and other information that Defendant may deem necessary to provide services and care.

35. Patients are required to provide and to otherwise entrust their PII and PHI to Defendant to receive healthcare services and, in return, they reasonably and appropriately expect that Atrium will safeguard their highly sensitive Private Information and keep it secure and confidential.

36. The information held by Defendant in its computer systems included the unencrypted Private Information of Plaintiff and Class Members.

37. Upon information and good faith belief, Defendant made promises and representations to its patients that the Private Information collected from them as a condition of obtaining healthcare services at Defendant would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

38. Due to the highly sensitive and personal nature of the information Atrium acquires and stores with respect to its patients, Atrium is required to keep patients' Private Information private; comply with industry standards related to data security and the maintenance of its patients' Private Information; inform its patients of its legal duties relating to data security and comply with

all federal and state laws protecting patients' Private Information; only use and release patients' Private Information for reasons that relate to the services it provides; and provide adequate notice to patients if their Private Information is disclosed without authorization.

39. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Atrium assumed legal and equitable duties it owed to them and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure and exfiltration.

40. Without the required submission of Private Information from Plaintiff and Class Members, Defendant could not perform the services it provides.

41. Plaintiff and Class Members relied on Atrium to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this Information, which Defendant ultimately failed to do.

42. Atrium's actions and inactions directly resulted in the Data Breach and the compromise of Plaintiff's and Class Members' Private Information.

B. Atrium Knew the Risks of Storing Valuable Private Information & the Foreseeable Harm to Victims.

43. Atrium was well aware that Private Information it collects is highly sensitive and of significant value to those who would use it for wrongful purposes.

44. Atrium also knew that a breach of its systems—and exposure of the information stored therein—would result in the increased risk of identity theft and fraud (financial and medical) against the individuals whose Private Information was compromised, as well as intrusion into their highly private health information.

45. These risks are not merely theoretical; in recent years, numerous high-profile data breaches have occurred at businesses such as Equifax, Facebook, Yahoo, Marriott, Anthem as well as countless ones in the healthcare industry.

46. PII has considerable value and constitutes an enticing and well-known target to hackers, who can easily sell stolen data as there has been a "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[10]

47. PHI, in addition to being of a highly personal and private nature, can be used for medical fraud and to submit false medical claims for reimbursement.[11]

48. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses and government entities.

49. In 2021 alone, there were 4,145 publicly disclosed data breaches, exposing 22 billion records. The United States specifically saw a 10% increase in the total number of data breaches.[12]

---

[10] Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/ (last visited Sept. 18, 2024).

[11] *See* Brian O'Connor, *Healthcare Data Breach: What to Know About them and What to Do After One*, Experian (June 14, 2018), https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/ (last visited Sept. 18, 2024).

[12] *Data Breach Report: 2021 Year End*, Risk Based Security (Feb. 4, 2022), https://www.riskbasedsecurity.com/2022/02/04/data-breach-report-2021-year-end/ (last visited Sept. 18, 2024).

50. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years; for instance, in 2017, 2.9 million people reported some form of identity fraud compared to 5.7 million people in 2021.[13]

51. The healthcare industry has become a prime target for threat actors: "High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks."[14]

52. Additionally, healthcare providers "store an incredible amount of patient data. Confidential data that's worth a lot of money to hackers who can sell it quickly – making the industry a growing target."[15]

53. Indeed, cybercriminals seek out PHI at a greater rate than other sources of personal information. In a 2022 report, the healthcare compliance company Protenus found that there were 905 medical data breaches in 2021, leaving over 50 million patient records exposed for 700 of the 2021 incidents. This is an increase from the 758 medical data breaches that Protenus compiled in 2020.[16]

---

[13] *Insurance Information Institute, Facts + Statistics: Identity theft and cybercrime*, Insurance Information Institute, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20 (last visited Sept. 18, 2024).

[14] *The healthcare industry is at risk*, SwivelSecure https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/ (last visited Sept. 18, 2024).

[15] *Id.*

[16] *2022 Breach Barometer*, https://www.protenus.com/breach-barometer-report (last visited Sept. 18, 2024).

54. The healthcare sector suffered about 337 breaches in the first half of 2022 alone according to Fortified Health Security's mid-year report released in July. The percentage of healthcare breaches attributed to malicious activity rose more than 5 percentage points in the first six months of 2022 to account for nearly 80 percent of all reported incidents.[17]

55. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including American Medical Collection Agency (25 million patients, March 2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020), Defendant knew or should have known that their electronic records would be targeted by cybercriminals.

56. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Defendant's patients especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud and more.

57. As indicated by Jim Trainor, former second in command at the FBI's cyber security division: "[m]edical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where PHI records can go from $20 say up to—we've even seen $60 or $70."[18]

---

[17] Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, Cybersecurity News (July 19, 2022), https://healthitsecurity.com/news/health-sector-suffered-337-healthcare-data-breaches-in-first-half-of-year (last visited Sept. 18, 2024).

[18] *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data*, *New Ponemon*

58. A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market whereas stolen payment card information sells for about $1.[19] According to Experian:

> Having your records stolen in a healthcare data breach can be a prescription for financial disaster. If scam artists break into healthcare networks and grab your medical information, they can impersonate you to get medical services, use your data open credit accounts, break into your bank accounts, obtain drugs illegally, and even blackmail you with sensitive personal details.
>
> ID theft victims often have to spend money to fix problems related to having their data stolen, which averages $600 according to the FTC. But security research firm Ponemon Institute found that healthcare identity theft victims spend nearly $13,500 dealing with their hassles, which can include the cost of paying off fraudulent medical bills.
>
> Victims of healthcare data breaches may also find themselves being denied care, coverage or reimbursement by their medical insurers, having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores. In the worst cases, they've been threatened with losing custody of their children, been charged with drug trafficking, found it hard to get hired for a job, or even been fired by their employers.[20]

59. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or

---

Study Shows, IDX (May 14, 2015), https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat (last visited Sept. 18, 2024).

[19] *Managing cyber risks in an interconnected world, Key findings from The Global State of Information Security® Survey 2015*, PriceWaterhouseCoopers, https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf (last visited Sept. 18, 2024).

[20] Brian O'Connor, *Healthcare Data Breach: What to Know About them and What to Do After One*, Experian (June 14, 2018), https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/ (last visited Sept. 18, 2024).

to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

60. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

61. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiff's and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiff and Class Members.

62. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a

freeze on their credit, and correcting their credit reports.[21] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

63. Identity thieves can also use stolen personal information such as Social Security numbers and PHI for a variety of crimes, including medical identity theft, credit card fraud, phone or utilities fraud, bank fraud, to obtain a driver's license or official identification card in the victim's name but with the thief's picture, to obtain government benefits, or to file a fraudulent tax return using the victim's information.

64. For example, Social Security numbers, which were compromised in the Data Breach, are among the worst kind of Private Information to have been stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as experienced by Plaintiffs and some Class Members, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[22]

65. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of

[21] *See* The FTC, https://www.identitytheft.gov/Steps (last visited Sept. 18, 2024).
[22] Social Security Administration, Identity Theft and Your Social Security Number, available at: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Sept. 18, 2024).

misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

66. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[23]

67. There may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or PHI is stolen and when it is misused.

68. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data has been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[24]

69. Even if stolen PII or PHI does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII and PHI about the individual, such as name, address, email address, and affiliations, to gain trust and

[23] Bryan Naylor, Victims of Social Security Number Theft Find It's Hard to Bounce Back, NPR (Feb. 9, 2015), available at: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited Sept. 18, 2024).

[24] U.S. Gov't Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: https://www.gao.gov/new.items/d07737.pdf (last visited Sept. 18, 2024).

increase the likelihood that a victim will be deceived into providing the criminal with additional information.

70. Based on the value of its patients' PII and PHI to cybercriminals, Defendant certainly knew the foreseeable risk of failing to implement adequate cybersecurity measures.

C. Atrium Breached its Duty to Protect its Patients' Private Information.

71. In or around April 29, 2024, Atrium learned that an unauthorized third party gained access to several employee email accounts via "phishing." Atrium allegedly began an investigation "immediately," and engaged a forensic consultant to assist with the investigation.[25] At that time, Atrium did not provide any details about the Data Breach whatsoever.

72. That investigation apparently confirmed that Atrium did suffer a phishing attack and the unauthorized third party "may have had access to the affected [email] accounts."[26]

73. Despite the investigation – that lasted about a month and a half – Atrium was not able to conclusively determine what the unauthorized third party viewed.

74. However, it appears highly likely that cybercriminals had access to and compromised patients' Private Information, including Social Security numbers, driver's license/state ID information, health and health insurance information, date of birth, financial and access information and other sensitive information.[27]

75. Upon information and good faith belief, Atrium finished its review of the impacted data in or about July 17, 2024.

---

[25] *See A Notice to our Patients*, *supra*, note 4.

[26] *Id*.

[27] *Id*.

76. Even though Defendant finished reviewing the impacted information around July 2024, Atrium did not begin notifying patients impacted by the Data Breach until on or about September 13, 2024 – or *four and a half months after the Data Breach*.

77. Even now Atrium still fails to disclose the true size of the Data Breach, refusing to provide the number of affected victims.

78. The Data Breach occurred as a direct result of Defendant's failure to implement and follow basic security procedures, and its failure to follow its own policies, in order to protect its patients' PII and PHI.

D. Atrium is Obligated Under HIPAA to Safeguard Private Information.

79. Atrium is required by HIPAA to safeguard patient PHI.

80. Atrium is an entity covered under HIPAA, which sets minimum federal standards for privacy and security of PHI.

81. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

82. Further to 45 C.F.R. § 160.103, HIPAA defines "protected health information" or PHI as "individually identifiable health information" that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium."

83. Under C.F.R. 160.103, HIPAA defines "individually identifiable health information" as "a subset of health information, including demographic information collected from an individual" that is (1) "created or received by a health care provider;" (2)"[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an

individual;" and (3) either (a) identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual."

84. HIPAA requires Atrium to: (a) ensure the confidentiality, integrity, and availability of all electronic PHI it creates, receives, maintains, or transmits; (b) identify and protect against reasonably anticipated threats to the security or integrity of the electronic PHI; (c) protect against reasonably anticipated, impermissible uses, or disclosures of the PHI; and (d) ensure compliance by its workforce to satisfy HIPAA's security requirements. 45 CFR § 164.102, *et. seq*.

85. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."[28]

86. While HIPAA permits healthcare providers to disclose PHI to third parties under certain circumstances, HIPAA does not permit healthcare providers to disclose PHI to cybercriminals nor did Plaintiff or the Class Members consent to the disclosure of their PHI to cybercriminals.

87. As such, Atrium is required under HIPAA to maintain the strictest confidentiality of Plaintiff's and Class Members' PHI that it requires, receives, and collects, and Defendant is further required to maintain sufficient safeguards to protect that information from being accessed by unauthorized third parties.

88. Given the application of HIPAA to Atrium, and that Plaintiff and Class Members entrusted their PHI to Defendant in order to receive healthcare services, Plaintiff and Class

[28] *Breach Notification Rule*, U.S. Dep't of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (last visited Sept. 18, 2024).

Members reasonably expected that Defendant would safeguard their highly sensitive information and keep their PHI confidential.

E. FTC Guidelines Prohibit Atrium from Engaging in Unfair or Deceptive Acts or Practices.

89. Atrium is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

90. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[29]

91. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[30]

92. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity

---

[29] *Start with Security – A Guide for Business*, United States Federal Trade Comm'n (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Sept. 18, 2024).

[30] *Protecting Personal Information: A Guide for Business*, United States Federal Trade Comm'n, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Sept. 18, 2024).

on the network; and verify that third-party service providers have implemented reasonable security measures.[31]

93. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

94. Atrium failed to properly implement basic data security practices. Atrium's failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PII and PHI constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

95. Atrium was at all times fully aware of its obligations to protect the PII and PHI of patients because of its position as a healthcare provider, which gave it direct access to reams of patient PII and PHI. Defendant was also aware of the significant repercussions that would result from its failure to do so.

F. The Monetary Value of Private Information.

96. As a result of Defendant's failures, Plaintiff and Class Members are at substantial increased risk of suffering identity theft and fraud or misuse of their Private Information.

97. From a recent study, 28% of consumers affected by a data breach become victims of identity fraud—this is a significant increase from a 2012 study that found only 9.5% of those affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identify fraud is only about 3%.[32]

---

[31] *Id.*

[32] Stu Sjouwerman, *28 Percent of Data Breaches Lead to Fraud*, KnowBe4, https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud (last visited

98. With respect to health care breaches, another study found "the majority [70%] of data impacted by healthcare breaches could be leveraged by hackers to commit fraud or identity theft."[33]

99. "Actors buying and selling PII and PHI from healthcare institutions and providers in underground marketplaces is very common and will almost certainly remain so due to this data's utility in a wide variety of malicious activity ranging from identity theft and financial fraud to crafting of bespoke phishing lures."[34]

100. The reality is that cybercriminals seek nefarious outcomes from a data breach and "stolen health data can be used to carry out a variety of crimes."[35]

101. Indeed, a robust "cyber black market" exists in which criminals openly post stolen Private Information on multiple underground Internet websites, commonly referred to as the dark web.

102. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information:

> The use of third-party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman

---

Sept. 18, 2024).

[33] Jessica David, *70% of Data Involved in Healthcare Breaches Increases Risk of Fraud*, HealthITSecurity, https://healthitsecurity.com/news/70-of-data-involved-in-healthcare-breachesincreases-risk-of-fraud (last visited Sept. 18, 2024).

[34] *Id.*

[35] Andrew Steger, *What Happens to Stolen Healthcare Data?*, HealthTech (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (last visited Sept. 18, 2024).

> [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[36]

103. Commissioner Swindle's 2001 remarks are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 Billion per year online advertising industry in the United States.[37]

104. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[38]

105. Recognizing the high value that consumers place on their Private Information, many companies now offer consumers an opportunity to sell this information.[39] The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will

---

[36] *Public Workshop: The Information Marketplace: Merging and Exchanging Consumer Data*, FED. TRADE COMM'N Tr. at 8:2-8 (Mar. 13, 2001), https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf (last visited Sept. 18, 2024).

[37] *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, The Wall Street Journal (Feb. 28, 2011), https://www.wsj.com/articles/SB10001424052748703529004576160764037920274.

[38] *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, FED. TRADE COMM'N (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.

[39] Angwin & Steel, *supra* note 38.

make a profit from their Private Information. This business has created a new market for the sale and purchase of this valuable data.

106. Consumers place a high value not only on their Private Information, but also on the privacy of that data. Researchers have begun to shed light on how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2014 was $1,349.[40]

107. The value of Plaintiff's and Class Members' Private Information on the black market is substantial. Sensitive health information can sell for as much as $363.[41]

108. This information is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

109. Health information in particular is likely to be used in detrimental ways—by leveraging sensitive personal health details and diagnoses to extort or coerce someone, and serious and long-term identity theft.[42]

110. "Medical identity theft is a great concern not only because of its rapid growth rate, but because it is the most expensive and time consuming to resolve of all types of identity theft.

---

[40] *See* U.S. Dep't of Justice, *Victims of Identity Theft,* OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf.

[41] Center for Internet Security, *Data Breaches: In the Healthcare Sector*, https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/.

[42] *Id.*

Additionally, medical identity theft is very difficult to detect which makes this form of fraud extremely dangerous."[43]

111. Medical identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[44]

112. The Federal Trade Commission has warned consumers of the dangers of medical identity theft, stating that criminals can use personal information like a "health insurance account number or Medicare number" to "see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care." The FTC further warns that instances of medical identity theft "could affect the medical care you're able to get or the health insurance benefits you're able to use[,]" while also having a negative impact on credit scores.[45]

---

[43] *The Potential Damages and Consequences of Medical Identity theft and Healthcare Data Breaches*, Experian, https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf (last visited Sept. 18, 2024).

[44] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, KAISER (Feb. 7, 2014) https://khn.org/news/rise-of-indentity-theft/.

[45] Federal Trade Commission, *What to Know About Medical Identity Theft*, What To Know About Medical Identity Theft | Consumer Advice (ftc.gov) (last visited Sept. 18, 2024).

113. Here, where health insurance information was among the Private Information impacted in the Data Breach, Plaintiff's and Class Members' risk of suffering future medical identity theft is especially substantial.[46]

114. The ramifications of Atrium's failure to keep its patients' Private Information secure are long-lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for 6 to 12 months or even longer.

115. Approximately 21% of victims do not realize their identity has been compromised until more than two years after it has happened.[47] This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[48]

116. Indeed, when compromised, healthcare related data is among the most private and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims

---

[46] *See* American Association of Retired Persons, *Watch for Medical Identity Theft*, https://www.aarp.org/money/scams-fraud/info-11-2010/watch_for_medical_wy.html#:~:text=Medical%20identity%20theft%20is%20when%20someone%20uses%20your,You%20can%20be%20harmed%20by%20medical%20identity%20theft (last visited Sept. 18, 2024).

[47] *See Medical ID Theft Checklist*, IDENTITYFORCE, https://www.identityforce.com/blog/medical-id-theft-checklist-2 (last visited Sept. 18, 2024).

[48] *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches*, EXPERIAN, (Apr. 2010), https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf.

were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[49]

117. Almost 50% of the surveyed victims lost their healthcare coverage as a result of the incident, while nearly 30% said their insurance premiums went up after the event. Forty percent of the victims were never able to resolve their identity theft at all. Seventy-four percent said that the effort to resolve the crime and restore their identity was significant or very significant. Data breaches and identity theft, including medical identity theft, have a crippling effect on individuals and detrimentally impact the economy as a whole.[50]

118. At all relevant times, Defendant was well-aware, or reasonably should have been aware, that the Private Information it maintains is highly sensitive and could be used for wrongful purposes by third parties, such as identity theft (including medical identity theft) and fraud.

119. Upon information and good faith belief, had Defendant remedied the deficiencies in its security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it would have prevented the ransomware attack into its systems and, ultimately, the theft of the Private Information of patients within its systems.

120. The compromised Private Information in the Data Breach is of great value to hackers and thieves and can be used in a variety of ways. Information about, or related to, an individual for which there is a possibility of logical association with other information is of great value to hackers and thieves.

---

[49] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/.

[50] *Id.*

121. Indeed, "there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII."[51] For example, different PII elements from various sources may be able to be linked in order to identify an individual, or access additional information about or relating to the individual.[52]

122. Based upon information and belief, the unauthorized parties have already utilized, and will continue utilize, the Private Information they obtained through the Data Breach to obtain additional information from Plaintiff and Class Members that can be misused.

123. In addition, as technology advances, computer programs may scan the Internet with wider scope to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible. This is known as the "mosaic effect."

124. Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

125. Thus, even if payment card information were not involved in the Data Breach, the unauthorized parties could use Plaintiff's and Class Members' Private Information to access accounts, including, but not limited to email accounts and financial accounts, to engage in the fraudulent activity identified by Plaintiffs.

---

[51] *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report*, FED. TRADE COMM'N 35-38 (Dec. 2010), https://www.ftc.gov/reports/preliminary-ftc-staff-report-protecting-consumer-privacy-era-rapid-change-proposed-framework.

[52] *See id.* (evaluating privacy framework for entities collecting or using consumer data with can be "reasonably linked to a specific consumer, computer, or other device").

126. Given these facts, any company that transacts business with customers and then compromises the privacy of customers' Private Information has thus deprived customers of the full monetary value of their transaction with the company.

127. In short, the Private Information exposed is of great value to hackers and cyber criminals and the data compromised in the Data Breach can be used in a variety of unlawful manners, including opening new credit and financial accounts in users' names.

G. Plaintiff & Class Members Have Suffered Compensable Damages.

128. For the reasons mentioned above, Defendant's conduct, which allowed the Data Breach to occur, caused Plaintiff and Class Members significant injuries and harm in several ways.

129. The risks associated with identity theft, including medical identity theft, are serious. While some identity theft victims can resolve their problems quickly, others spend hundreds to thousands of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

130. In order to mitigate against the risks of identity theft and fraud, Plaintiff and members of the Class must immediately devote time, energy, and money to: 1) closely monitor their medical statements, bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

131. Once Private Information is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives as a result of Defendant's conduct.

132. Further, the value of Plaintiff and Class Members' PII and PHI has been diminished by its exposure in the Data Breach.

133. Plaintiff and Class Members now face a greater risk of identity theft, including medical and financial identity theft.

134. Plaintiff and Class Members are also at a continued risk because their information remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as Defendant fails to undertake the necessary and appropriate security and training measures to protect its patients' PII and PHI.

135. Plaintiff and Class Members have suffered emotional distress as a result of the Data Breach, the increased risk of identity theft and financial fraud, and the unauthorized exposure of their private medical information to strangers.

136. Plaintiff and Class Members also did not receive the full benefit of their bargain when paying for medical services. Instead, they received services of a diminished value to those described in their agreements with Defendant. Plaintiff and Class Members were damaged in an amount at least equal to the difference in the value between the services they thought they paid for (which would have included adequate data security protection) and the services they actually received.

137. Plaintiff and Class Members would not have obtained services from Atrium had they known that Defendant failed to properly train its employees, lacked safety controls over its

computer network, and did not have proper data security practices to safeguard their Private Information from criminal theft and misuse.

138. Finally, in addition to a remedy for the economic harm, Plaintiff and Class Members maintain an undeniable interest in ensuring that their Private Information remains secure and is not subject to further misappropriation and theft.

REPRESENTATIVE PLAINTIFF'S EXPERIENCE

Plaintiff Kirksey

139. Beginning in or around 2020, Plaintiff Kirksey started to utilize Atrium for healthcare services.

140. While seeking those services and treatments, Atrium required Plaintiff to provide—and Plaintiff provided—Private Information including her first and last name, birth date, email address, phone number and reason for visit.

141. Upon becoming a patient, Plaintiff was asked by Defendant to provide additional personal information including her Social Security number, health insurance, and financial information.

142. To her knowledge, Plaintiff has never been the victim of a prior data breach.

143. As a direct result of the Data Breach, Plaintiff has suffered or will imminently suffer injury from the unauthorized disclosure and misuse of her Private Information that can be directly traced to Defendant.

144. On information and belief, Plaintiff's Private Information unauthorizedly disclosed in the Data Breach is now in the possession of cybercriminals and/or on the Dark Web where it can be sold and utilized for fraudulent and criminal purposes.

145. In addition, Plaintiff must now spend time and effort attempting to remediate the harmful effects of the Data Breach, including monitoring their credit reports, and fears for their personal financial security and uncertainty over the information compromised in the Data Breach. She is experiencing feelings of anxiety, sleep disruption, stress, and fear because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

146. Plaintiff was highly disturbed by the Data Breach's nature and the thought of cybercriminals accessing her highly sensitive Private Information and the harm caused by the Data Breach.

147. As a result of Atrium's Data Breach, Plaintiff faces a lifetime risk of additional identity theft, as it includes sensitive information that cannot be changed, like her Social Security number.

CLASS ALLEGATIONS

148. Plaintiff brings this class action on behalf of herself and all other individuals who are similarly situated pursuant to Rule 23 of the Federal Rules of Civil Procedure.

149. Plaintiff seeks to represent a Nationwide Class of persons to be defined as follows:

> **All individuals in the United States whose PII and/or PHI was compromised in the Atrium Data Breach which occurred in or about April 2024 and was announced in September 2024 (the "Nationwide Class").**

150. Excluded from the Class are Defendant, its subsidiaries and affiliates, officers and directors, any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

151. This proposed class definition is based on the information available to Plaintiff at this time. Plaintiff may modify the class definition in an amended pleading or when she moves for class certification, as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

152. **Numerosity:** Plaintiff is informed and believes, and thereon alleges, that there are at minimum, thousands of members of the Class described above. The exact size of the Class and the identities of the individual members are identifiable through Defendant's records, including but not limited to the files implicated in the Data Breach, but based on public information, the Class includes thousands of individuals, if not substantially more.

153. **Commonality:** This action involved questions of law and fact common to the Class. Such common questions include but are not limited to:

a. Whether Defendant failed to timely notify Plaintiff and Class Members of the Data Breach;

b. Whether Defendant had a duty to protect the PII and PHI of Plaintiff and Class Members;

c. Whether Defendant was negligent in collecting and storing Plaintiff's and Class Members' PII and PHI, and breached its duties thereby;

d. Whether Defendant entered into an implied contract with Plaintiff and Class Members;

e. Whether Defendant breached that contract by failing to adequately safeguard Plaintiff's and Class Members' PII and PHI;

f. Whether Defendant was unjustly enriched;

g. Whether Plaintiff and Class Members are entitled to damages as a result of Defendant's wrongful conduct; and

h. Whether Plaintiff and Class Members are entitled to declaratory judgment due to Defendant's wrongful conduct.

154. **Typicality:** Plaintiff's claims are typical of the claims of the members of the Class. The claims of the Plaintiff and members of the Class are based on the same legal theories and arise

from the same unlawful and willful conduct. Plaintiff and members of the Class were all patients, or family members or caregivers of patients, of Defendant, each having their PII and PHI exposed and/or accessed by an unauthorized third party.

155. **Adequacy of Representation:** Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the members of the Class. Plaintiff will fairly, adequately, and vigorously represent and protect the interests of the members of the Class and have no interests antagonistic to the members of the Class. In addition, Plaintiff has retained counsel who are competent and experienced in the prosecution of class action litigation. The claims of Plaintiff and the Class Members are substantially identical as explained above.

156. **Superiority:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense, and promote uniform decision-making.

157. **Predominance:** Common questions of law and fact predominate over any questions affecting only individual Class Members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendant's liability and the fact of damages is common to Plaintiff and each member of the Class. If Defendant breached its duty to Plaintiff and Class Members, then Plaintiff and each Class member suffered damages by that conduct.

158. **Injunctive Relief:** Defendant has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. Civ. P. 23 (b)(2).

159. **Ascertainability:** Members of the Class are ascertainable. Class membership is defined using objective criteria and Class Members may be readily identified through Defendant's books and records.

CAUSES OF ACTION

COUNT I

NEGLIGENCE
(On behalf of Plaintiff & the Nationwide Class)

160. Plaintiff restates and realleges all preceding factual allegations above as if fully set forth herein.

161. Plaintiff brings this claim individually and on behalf of the Class.

162. Defendant owed a duty under common law to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII and PHI in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

163. Defendant's duty to use reasonable care arose from several sources, including but not limited to those described below.

164. Defendant had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of the Defendant. By collecting and storing valuable PII and PHI that is routinely targeted by criminals for unauthorized access, Defendant was obligated to act with reasonable care to protect against these foreseeable threats.

165. Defendant's duty also arose from Defendant's position as a healthcare provider. Defendant holds itself out as a trusted provider of healthcare, and thereby assumes a duty to reasonably protect its patients' information. Indeed, Defendant was in a unique and superior position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

166. Defendant's duties also arose from statutes applicable to Defendant designed to prevent the harm that Plaintiff and Class Members suffered and will continue to suffer.

167. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by entities such as Defendant or failing to use reasonable measures to protect PII and PHI. Various FTC publications and orders also form the basis of Defendant's duty.

168. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and PHI and not complying with the industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII and PHI they obtained and stored and the foreseeable consequences of a data breach involving PII and PHI of its patients.

169. Plaintiff and members of the Class are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

170. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

171. Atrium is an entity covered under HIPAA which sets minimum federal standards for privacy and security of PHI.

172. Pursuant to HIPAA, 42 U.S.C. § 1302d, *et. seq.*, and its implementing regulations, Defendant had a duty to implement and maintain reasonable and appropriate administrative, technical, and physical safeguards to protect Plaintiff's and the Class Members' electronic PHI.

173. Specifically, HIPAA required Defendant to: (a) ensure the confidentiality, integrity, and availability of all electronic PHI it creates, receives, maintains, or transmits; (b) identify and protect against reasonably anticipated threats to the security or integrity of the electronic PHI; (c) protect against reasonably anticipated, impermissible uses, or disclosures of the PHI; and (d) ensure compliance by their workforce to satisfy HIPAA's security requirements. 45 C.F.R. § 164.102, *et. seq*.

174. Defendant violated HIPAA by actively disclosing Plaintiff's and the Class Members' electronic PHI and by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PHI.

175. Plaintiff and the Class Members are patients within the class of persons HIPAA was intended to protect.

176. Defendant's violation of HIPAA constitutes negligence *per se*.

177. The harm that has occurred as a result of Defendant's conduct is the type of harm that the FTC Act and HIPAA were intended to guard against.

178. As a direct and proximate result of Defendant's negligence, Plaintiff's and Class Members have been injured as described herein and in Paragraph 96 above, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

179. Defendant breached the duties owed to Plaintiff and Class Members and thus was negligent. As a result of a successful attack directed towards Defendant that compromised Plaintiff's and Class Members' PII and PHI, Defendant breached its duties through some combination of the following errors and omissions that allowed the data compromise to occur: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks

to the security, confidentiality, and integrity of patient information that resulted in the unauthorized access and compromise of PII and PHI; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to its patients; and (h) failing to adequately train and supervise employees and third party vendors with access or credentials to systems and databases containing sensitive PII or PHI.

180. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their PII and PHI would not have been compromised.

181. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered injuries, including:

a. Theft of their PII and/or PHI;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;

g. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data;

i. Future costs in terms of time, effort, and money that will be expended as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members;

j. The diminished value of the services they paid for and received and

k. Emotional distress from the unauthorized disclosure of PII and PHI to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class Members.

182. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

COUNT II

BREACH OF IMPLIED CONTRACT
(*On behalf of Plaintiff & the Nationwide Class*)

183. Plaintiff restates and realleges all preceding factual allegations above as if fully set forth herein.

184. Plaintiff brings this claim individually and on behalf of the Class.

185. When Plaintiff and Class Members provided their PII and PHI to Atrium, they entered into implied contracts with Defendant, under which Defendant agree to take reasonable steps to protect Plaintiff's and Class Members' PII and PHI, comply with its statutory and common law duties to protect Plaintiff's and Class Members' PII and PHI, and to timely notify them in the event of a data breach.

186. Atrium solicited and invited Plaintiff and Class Members to provide their PII and PHI as part of Defendant's provision of healthcare services. Plaintiff and Class Members accepted Defendant's offers and provided their PII and PHI to Defendant.

187. Implicit in the agreement between Plaintiff and Class Members and Atrium, was Defendant's obligation to: (a) use such PII and PHI for business purposes only; (b) take reasonable steps to safeguard Plaintiff's and Class Members' PII and PHI; (c) prevent unauthorized access and/or disclosure of Plaintiff's and Class Members' PII and PHI; (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or disclosure of their PII and PHI; (e) reasonably safeguard and protect the PII and PHI of Plaintiff and Class Members from unauthorized access and/or disclosure; and (f) retain Plaintiff's and Class Members' PII and PHI under conditions that kept such information secure and confidential.

188. When entering into implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with its statutory and common law duties to adequately protect Plaintiff's and Class Members' PII and PHI and to timely notify them in the event of a data breach.

189. Plaintiff and Class Members paid money to Defendant in exchange for services, along with Defendant's promise to protect their PII and PHI from unauthorized access and

disclosure. Plaintiff and Class Members reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Atrium failed to do so.

190. Plaintiff and Class Members would not have provided their PII and PHI to Atrium had they known that Defendant would not safeguard their PII and PHI, as promised, or provide timely notice of a data breach.

191. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

192. Atrium breached its implied contracts with Plaintiff and Class Members by failing to safeguard their PII and PHI and by failing to provide them with timely and accurate notice of the Data Breach

193. The losses and damages Plaintiff and Class Members sustained, include, but are not limited to:

a. Theft of their PII and/or PHI;

b. Costs associated with purchasing credit monitoring and identity theft protection services;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII and PHI;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;

g. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data;

i. Future costs in terms of time, effort, and money that will be expended as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members;

j. The diminished value of the services they paid for and received; and

k. Emotional distress from the unauthorized disclosure of PII and PHI to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class Members.

194. As a direct and proximate result of Atrium's breach of contract, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

195. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (1) strength its data security systems and monitoring procedures; (2) submit to future annual audits of those systems and monitoring procedures; and (3) immediately provide and continue to provide adequate credit monitoring to Plaintiff and all Class Members.

COUNT III

BREACH OF THE IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING
(*On behalf of Plaintiff & the Nationwide Class*)

196. Plaintiff restates and realleges all preceding factual allegations above as if fully set forth herein.

197. Plaintiff brings this claim individually and on behalf of the Class.

198. Every contract in this State has an implied covenant of good faith and fair dealing. This implied covenant is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

199. Plaintiff and Class Members have complied with and performed all conditions of their contracts with Defendant.

200. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard Private Information, failing to timely and accurately disclose the Data Breach to Plaintiff and Class Members, and continued acceptance of and storage of Private Information after Defendant knew or should have known of the security vulnerabilities of the systems that were exploited in the Data Breach.

201. Defendant acted in bad faith and/or with malicious motive in denying Plaintiffs and Class Members the full benefit of their bargains as originally intended by the parties, thereby causing them injury in an amount to be determined at trial.

COUNT IV

UNJUST ENRICHMENT
(*On behalf of Plaintiff & the Nationwide Class*)

202. Plaintiff brings this claim individually and on behalf of the Class in the alternative to the Second Cause of Action above.

203. Upon information and belief, Defendant funds its data security measures from its general revenue including payments made by or on behalf of Plaintiff and Class Members.

204. As such, a portion of the payments made by or on behalf of Plaintiff and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

205. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased healthcare services from Defendant and/or its agents and in so doing provided Defendant with their PII and PHI.

206. In exchange, Plaintiff and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their PII and PHI protected with adequate data security.

207. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII and PHI of Plaintiff and Class Members for business purposes.

208. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members PII and PHI. Instead of providing a reasonable level of data security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits and the expense of Plaintiff and Class Members by utilizing cheaper, ineffective data security measures.

209. Under the principles of equity and good conscience, Atrium should not be permitted to retain the money belonging to Plaintiff and Class Members because Defendant failed to implement appropriate data management and security measures that are mandated by its common law and statutory duties.

210. Defendant failed to secure Plaintiff and Class Members' PII and PHI and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members conferred upon Atrium.

211. Defendant acquired Plaintiff's and Class Members' PII and PHI through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

212. If Plaintiff and Class Members knew that Defendant had not reasonably secured their PII and PHI, they would not have agreed to provide their PII and PHI to Defendant.

213. Plaintiff and Class Members have no adequate remedy at law.

214. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered injuries, including:

a) Theft of their PII and/or PHI;

b) Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

c) Costs associated with purchasing credit monitoring and identity theft protection services;

d) Lowered credit scores resulting from credit inquiries following fraudulent activities;

e) Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f) The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;

g) Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

h) Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data;

i) Future costs in terms of time, effort, and money that will be expended as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members;

j) The diminished value of the services they paid for and received; and

k) Emotional distress from the unauthorized disclosure of PII and PHI to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class Members.

215. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and noneconomic losses.

216. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

COUNT V

DECLARATORY JUDGMENT
(*On behalf of Plaintiff & the Nationwide Class*)

217. Plaintiff restates and realleges all preceding allegations above as if fully set forth herein.

218. Plaintiff brings this claim individually and on behalf of the Class.

219. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those

here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

220. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' PII and PHI and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff's and Class Members from further data breaches that compromise their PII and PHI. Plaintiff alleges that Defendant's data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of her PII and PHI and remains at imminent risk that further compromises of her PII and PHI will occur in the future.

221. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owes a legal duty to secure patients' PII and PHI and to timely notify patients of a data breach under the common law, Section 5 of the FTC Act, and HIPAA; and

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure patients' PII and PHI.

222. This Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards to protect patients' PII and PHI.

223. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendant.

224. The risk of another such breach is real, immediate and substantial.

225. If another breach at Defendant occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

226. The hardship to Plaintiff if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

227. Issuance of the requested injunction will not disserve the public interest. In contrast, such an injunction would benefit the public by preventing another data breach at Defendant, thus eliminating the additional injuries that would result to Plaintiff and Class Members whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the proposed Nationwide Class, respectfully requests that this Court enter an Order:

a) Certifying this case as a class action on behalf of the Nationwide Class and State Class defined above, appointing Plaintiff as representative of the Class, and appointing her counsel as Class Counsel;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or unauthorized disclosure of Plaintiff's and Class Members' Private Information;

c) For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members;

d) For an award of damages, including but not limited to, actual, consequential, punitive, and nominal damages, as allowed by law in an amount to be determined;

e) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

f) Pre- and post-judgment interest on any amounts awarded;

g) Such other and further relief as this Court may deem just and proper;

h) For trial by jury.

Date: September 18, 2024

Respectfully submitted,

/s/ David M. Wilkerson

David M. Wilkerson
N.C. Bar No. 35742
THE VAN WINKLE LAW FIRM
11 N Market Street
Asheville, NC 28801
Ph: (828) 258-2991
dwilkerson@vwlawfirm.com

Attorney for Plaintiff & Putative Class